Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 20 June 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- MasterCard International announced Friday that a computer hacker may have accessed more than 40 million credit card accounts at CardSystems Solutions, in what could be the largest in a series of recent security breaches involving consumer data. (See item 3)
- The Canadian Press reports an infectious disease expert says policy makers should start intensive planning since an influenza pandemic would dramatically disrupt the processing and distribution of food supplies across the world. (See item 22)
- The American Water Works Association has published a new report that identifies active and effective practices for securing water supplies and will help utilities implement security practices and measure their effectiveness. (See item 23)

DHS/IAIP Update *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 16, ReliabilityFirst Corporation* — **Regional electric reliability councils form.** Four regional electric reliability councils took another major step toward creating a new, larger electric reliability council in the Mid−Atlantic and Central United States by forming ReliabilityFirst Corporation. ReliabilityFirst was organized as a Delaware corporation on June 15, 2005. ReliabilityFirst's goal is to preserve and enhance electric service reliability and

security of infrastructure for the interconnected electric system in its region. Upon approval by the North American Electric Reliability Council (NERC), ReliabilityFirst will replace three existing regional councils, the East Central Area Reliability Council (ECAR), Mid−America Interconnected Network (MAIN) and Mid−Atlantic Area Council (MAAC). A fourth council, the Midwest Reliability Organization (MRO), is also participating in the project. However, MRO is not part of the initial combination. The key functions of ReliabilityFirst will be the development of regional standards for reliable planning and operation of the electric utility system and non−discriminatory compliance monitoring and enforcement of standards in its region.
ReliabilityFirst initiative: http://www.maac−rc.org/rrcboundaries
Source: http://www.maac−rc.org/rrcboundaries/downloads/20050617−reliability−first−news−release.pdf

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *June 16, Express−News (San Antonio, TX)* — **Mysterious empty 50−gallon drum forces evacuation in Texas neighborhood.** More than 75 Terrell Hills, TX residents evacuated their homes Thursday morning, June 16, after a mysterious 50−gallon drum, along with a threatening note, was left in a driveway. Firefighters who responded noticed a marking on the drum that indicated it might contain hazardous materials. A two−block radius was evacuated about 10 a.m. as authorities tried to determine the drum's contents. A military explosives expert used a specially designed robot to determine, without opening the drum, that there were no explosives inside. Members of a hazardous materials team were placing the drum in a leak−proof container when they realized it was empty. Terrell Hills Police Sgt. Rick Trevino said it appears the barrel was deliberately placed in the driveway. Trevino would not reveal what the note said, but he indicated it "could be construed as threatening." He did not discuss possible motives, other than to rule out a domestic disturbance. "We do know who left it, and any and all appropriate charges (will) be filed against the perpetrator," he said.
Source: http://www.mysanantonio.com/news/metro/stories/MYSA061605.en.terrellhilld.16fb693c.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *June 18, Associated Press* — **Millions of credit card accounts could be affected by computer hack.** A computer hacker may have accessed more than 40 million credit card accounts in what could be the largest in a series of recent security breaches involving consumer data, officials said. MasterCard International Inc. announced Friday, June 17, that the breach

was traced to Atlanta−based CardSystems Solutions Inc., which processes credit card and other payments for banks and merchants. All brands of credit cards could be affected. The compromised data did not include addresses or Social Security numbers, said MasterCard spokesperson Sharon Gamsin. The data that may have been viewed −− names, banks and account numbers −− could be used to steal funds, but not identities. Gamsin said she did not know how the virus−like computer script that captured customer data got into CardSystems' network, which MasterCard said was infiltrated by an "unauthorized individual." MasterCard said 14 million of its customers may have been exposed to fraud. A spokesperson for American Express said a small number of its cardholders were affected, but would not give an exact number. Discover Financial Services Inc. wouldn't say whether its customers were affected. Visa USA and a large issuer of cards, MBNA Corp., did not return calls for comment. The FBI is investigating.
Source: http://news.yahoo.com/news?tmpl=story&u=/ap/20050618/ap_on_bi_ge/credit_cards_breach

4. *June 17, Financial Times* — **Washington urged to adopt standard on identity theft.** The chairman of the Federal Trade Commission (FTC) on Thursday, June 16, encouraged lawmakers to adopt a federal notification standard that would force companies to alert consumers if a data breach had caused “significant” risk of identity theft. However, they stopped short of recommending a restriction on the sale of Social Security numbers. Deborah Majoras, FTC chair, also told the Senate commerce committee she did not support the creation of an office of identity theft within the FTC, which some lawmakers suggested, if it were specifically designed to assist identity−theft victims. Majoras said one of the toughest questions facing the FTC was how it would determine whether or not a data breach constituted a significant enough threat to consumers to warrant forced notification. Majoras' testimony coincided with an announcement by the FTC that it had reached a settlement with BJ's Wholesale, a leading U.S. warehouse retailer, over charges that the company's failure to take appropriate security measures to protect its customers' sensitive information was an unfair practice and violation of federal law. BJ's was not required to pay a fine as part of the settlement, but will be required to establish a security program that includes administrative, technical and physical safeguards.
Source: http://news.ft.com/cms/s/b7a16eac−df12−11d9−84f8−00000e2511c 8.html

5. *June 17, Chicago Tribune* — **Illinois consumers to get news of potential identity theft.** Businesses will be required to notify Illinois customers quickly when a security failure threatens the confidentiality of personal information, under a new law signed Thursday, June 16, by Governor Rod Blagojevich. Passed in the wake of several corporate security breaches around the country, the law will "provide consumers some peace of mind and protection from the fastest growing crime in the country, identity theft," Blagojevich said. Illinois is the second state to pass such a law.
Personal Information Protection Act:
http://www.ilga.gov/legislation/94/HB/PDF/09400HB1633lv.pdf
Source: http://www.chicagotribune.com/news/local/nearwest/chi−050617 0195jun17,1,1110666.story?coll=chi−newslocalnearwest−hed&ctr ack=2&cset=true

6. *June 16, Knight Ridder Tribune* — **Two charged in national credit card skimming case.** Two former waiters from a popular North Carolina restaurant have been charged in a national

skimming case in which authorities say more than 650 credit card numbers were stolen and sold for about $25 a pop. Federal and state authorities arrested Benjamin Christopher Gadson, who also uses Townsend as a surname, and Juan Alexander Canales on Tuesday, June 14, and charged each with three counts of financial card theft, court records show. Authorities say the ring extended as far as Florida, Missouri and California and represents a growing trend in identity theft that even the most cautious consumer might not be able to avoid. The two men are accused of stealing the credit card information while working as waiters at the Outback Steakhouse in Matthews, NC, from late 2003 until mid−2004, said Daniel Paulson, the acting special agent−in−charge for the North Carolina office of the U.S. Secret Service.
Source: http://www.kansascity.com/mld/kansascity/news/nation/1191340 3.htm

7. *June 16, Internet Retailer* — **As phishing attacks spread, retailers are lax in fighting them, expert says.** E−mail phishing attacks claim more than 2,000 victims per day and steal close to $1 billion a year, but many retailers fall short of taking basic steps to prevent them, Dave Jevans says, chairman of the Anti−Phishing Working Group (APWG). Website operators and brand owners can take several steps to prevent phishing attacks from occurring and to mitigate their impact on consumers when they do occur, Jevans says. For example, one of the most effective means of mitigating the impact of phishing attacks, Jevans says, is through consumer education. Retailers should place on their Websites information about how to recognize phishing e−mails and about how to contact the retailer to check on a suspected phishing e−mail, he adds. However, not enough retailers are taking such preventive actions, and in some cases are even doing things that indirectly support phishing, Jevans says. He cites one major brand that sent out a large amount of marketing e−mails from a domain other than its own branded domain −− a format that made its e−mail appear like a phishing attack. “If you keep sending e−mail that looks like phishing, you’re training your customers to respond to phishing,” Jevans says. “We’ve seen quite a lot of retailers doing that.”
Anti−Phishing Working Group: http://www.antiphishing.org
Source: http://internetretailer.com/dailyNews.asp?id=15248

8. *June 16, Internet Retailer* — **Pharming, phishing remain major online fraud threats, VeriSign says.** Pharming, in which hackers intercept personal data sent between a shopper and a genuine Website, is emerging as a major method of online fraud, according to VeriSign Inc.’s most recent Internet Security Intelligence Briefing. The briefing is based on transactions settled by VeriSign during the first quarter. VeriSign also found that phishing remains a major threat to Website security, with phishers using increasingly sophisticated technology. Recent phishing attacks are exploiting technical flaws in software. One technique uses malicious software, known as malware, which monitors what a user types and forwards the information to the hacker. Malware can be installed through viruses, worms or Trojan horses and is often included with downloaded software. “These attacks require a far higher level of technical sophistication than social engineering attacks, but can be much harder to detect,” VeriSign says. In its review of first−quarter transactions, VeriSign also discovered that 84.9% of attempted fraudulent transactions originated in the U.S. Canada was second with 5.2%, followed by Great Britain (1.1%), Australia and Germany (0.9%), and Japan (0.7%).
Internet Security Intelligence Briefing: http://www.verisign.com/static/030910.pdf
Source: http://internetretailer.com/dailyNews.asp?id=15253

9.

June 16, CNET News.com — **Canadian credit agency reports data breach.** The credit files of about 600 Canadian consumers were accessed without authorization, credit reporting agency Equifax Canada said Thursday, June 16. The breach resulted from what appears to be improper use of the access codes and passwords of one of Equifax's customers, the company said in a statement. Most of the affected people are in British Columbia, Canada, and all have been contacted and offered a one−year subscription to a credit monitoring service, Equifax said.
Source: http://news.zdnet.com/2110−1009_22−5750434.html

[Return to top]

Transportation and Border Security Sector

10. *June 19, Daily Herald (UT)* — **Regional aviation on the rise.** The added security after the terrorist attacks of September 11, 2001, has had an unexpected positive effect on the general aviation industry and Utah's regional airports in particular. The extra inconvenience has caused more and more businesses to turn to privately owned planes to move their employees around the country, and those planes are seeking smaller airports at which to land. Combine that growth with the increased flight schools and helicopter landing schools in the Utah valley area and airports like Provo Municipal, Ogden−Hinckley and Nephi Municipal are seeing an upswing in operations. Pat Morley, director of the Utah Department of Transportation's Division of Aeronautics, said the business jet sector is growing substantially, which has fueled much of the growth in smaller airports. Ed Rich, general manager of the Ogden−Hinckley Airport, said he has seen a significant increase in the number of business jets coming through his airport, particularly since 9/11 and the added hassle of commercial airports. Ogden's proximity to Salt Lake City makes it a reliever airport for Salt Lake International Airport any time weather or other adverse conditions make landing in Salt Lake difficult. The goal for Ogden−Hinckley is to remain viable, continue serving current customers, and look into bringing some commercial flights in the near future.
Source: http://www.harktheherald.com/modules.php?op=modload&name=News&file=article&sid=57703&mode=thread&order=0&thold=0

11. *June 18, Buffalo News (NY)* — **Criticized camera system works on Canadian border.** In Buffalo, NY, federal agents who use the U.S. Border Patrol's border camera system every day say it has provided a big boost to border surveillance efforts in Youngstown, Lewiston, and Niagara Falls. Yet plans for an extensive network of security camera towers stretching from Youngstown to Hamburg, NY, have been put on hold because of a congressional investigation into the Border Patrol's Integrated Surveillance Intelligence System. The system, comprising sensors and cameras mounted on tall towers along the Canadian and Mexican borders, was supposed to upgrade security. But the government says mechanical breakdowns and questionable financial practices have left the system in disarray. However, the four camera towers in use in New York's Niagara County are doing just fine. "Each of these cameras allows us to scan an area that would take four or five agents to keep an eye on," Ed Duda, deputy chief of patrol for the Border Patrol's Buffalo sector. "It's especially effective at night, when we use the infrared cameras." The local towers were installed between 2002 and 2004 under the nationwide Border Patrol program. All the towers are at least 50 feet tall.
Source: http://www.buffalonews.com/editorial/20050618/1017098.asp

12. *June 17, Government Technology* — **Iris−scan authentication cuts fraud in Connecticut vehicle emissions testing.** With the help of increasingly sophisticated digital imaging techniques, advanced software processing algorithms, and faster computing speeds, the measurement of human biometrics has become a practical tool applicable to everyday system user authentication. For example, in October of 2003 Applus+ Technologies, Inc. pioneered the first ever application of an iris scanning authentication system in a vehicle emissions inspection program. Under contract to Connecticut's Department of Motor Vehicles (DMV), Applus+ provides the iris scan system to 270 independent inspection and repair facilities to authenticate some 1300 licensed inspectors before each and every government−mandated vehicle inspection. Approximately 900,000 vehicles are inspected via that system each year. Applus+ provided each of the private inspection stations a complete set of computerized emissions analysis equipment, including the integral iris authentication camera and its associated software. The Connecticut DMV performs its own internal audit of the authentication procedures and they give the iris−scan technology high marks. Tim Kulish, the Division Manager for Connecticut DMV's Emissions Division reports that, "This technology and our internal audit procedures have virtually eliminated authentication violations that were commonplace with the badge−and−pass code verification system."
Source: http://www.govtech.net/news/news.php?id=94298

13. *June 17, Associated Press* — **American Airlines trying to burn less fuel.** American Airlines believes it can save $45 million on jet fuel this year by urging pilots and other employees to focus on conservation. Among the steps the nation's largest airline is taking are refueling at airports where fuel is cheapest, reducing fuel burn while jets are parked at gates, and carrying less water to reduce weight and increase mileage. American launched an internal Internet site this week to detail its "Fuel Smart" program. It wants pilots, dispatchers, mechanics and others to attempt, together, to save fuel. Fuel accounts for about 20% of an airline's costs, second behind only labor. "With the sudden and catastrophic rise in fuel costs over the past year, a more intensive approach to fuel conservation is necessary," Chairman and Chief Executive Gerard Arpey wrote in a memo to employees.
Source: http://www.usatoday.com/travel/news/2005−06−16−american−fuel −conserve_x.htm

14. *June 17, USA TODAY* — **US Airways' retention plan gets partial approval.** A bankruptcy judge on Thursday, June 16, gave US Airways' management a partial victory in its bid to spend millions on incentives to keep key employees from leaving. Judge Stephen Mitchell, who is presiding over the airline's bankruptcy case in Alexandria, VA, effectively nixed so−called "golden parachutes" for top executives while allowing the financially struggling carrier to spend up to about $28 million to keep a broad swath of key workers on the job. Mitchell's approval permits severance packages and retention bonuses for about 1,800 managers and key employees while the airline works toward its planned merger with Tempe, AZ−based America West. But Mitchell rejected US Airways' request to give its top 25 officers new contracts containing lucrative severance agreements. Mitchell ruled that US Airways must deal with that issue in its forthcoming reorganization plan, giving creditors a say. Rank−and−file workers at the USA's No. 7 airline have taken deep pay cuts during two rounds of bankruptcy reorganization. Mitchell said some spending on bonuses is necessary in light of recent departures. US Airways has 340 open management positions. "The company is experiencing a serious exodus of management employees that threatens its ability to reorganize," Mitchell wrote in a 15−page opinion.

Source: http://www.usatoday.com/travel/news/2005−06−16−usairways−usa t_x.htm

15. *June 17, National Journal* — **Efforts to combat nuclear terrorism hindered by porous borders.** As director of operations and emergency management for the Port of Los Angeles, Noel Cunningham is responsible for securing a facility which, together with the neighboring Port of Long Beach, is the gateway for 44 percent of the goods that come into the United States. A bomb that gets through this port is just a drive down the highway from any city in 48 states. Cunningham's security challenge is hardly unique: America's porous borders and winding coastlines are impossible to fortify completely. Three thousand trucks roll through the Otay Mesa border crossing in Southern California each day. In October, the Otay Mesa crossing got its batch of radiation portal monitors, which look like enormous stereo speakers with bright−yellow borders. As trucks exit the tollbooth−like border checkpoints, they drive through the monitors at regular speed. The monitors beep when they detect radiation. All things considered, the most promising defense is a network of intelligence −− both high−tech and human −− to spot suspicious anomalies while they are as far away from America as possible. For example, across the ocean in the port of Hong Kong, a pilot project is under way to scan every cargo container for nuclear material.
Source: http://www.govexec.com/dailyfed/0605/061705nj1.htm

16. *June 17, Associated Press* — **Second helicopter crashes in New York.** A corporate helicopter plunged into the East River just blocks south of the United Nations on Friday, June 17, the second helicopter crash in four days in the waters off Manhattan. Rescuers pulled all eight on board out of the choppy water. Two pilots and six businessmen, who work for MBNA Corp., were aboard the Sikorsky S−76 when it went down seconds after taking off from the 34th Street heliport. The chopper made it barely one block north before it suddenly tumbled tail−first into the water. The cause of the crash was not immediately known. The helicopter sank afterward and was later pulled from the river using a 20−ton crane. The National Transportation Safety Board plans to investigate the crash. On Tuesday, June 14, another helicopter crashed into the East River shortly after takeoff for a sightseeing flight. Six tourists and the pilot were hospitalized.
Source: http://www.cnn.com/2005/US/06/17/helicopter.crash.ap/index.h tml

[Return to top]

Postal and Shipping Sector

17. *June 17, Santa Cruz Sentinel (CA)* — **Meningitis delivery costs U.S. Postal Service.** A family has settled a lawsuit against the U.S. Postal Service after a package they received in the mail from their daughter was found to have been exposed to potentially deadly bacterial meningitis. Serena Lewis mailed three boxes from New York to her parents' home in May 2001, according to a family attorney. Two packages arrived safely unopened, but her parents discovered a biohazard vial tucked between Lewis' socks, shoes, and CDs in a third box. Shaana Rahman, a family lawyer, said the meningitis container came from a damaged package sent via the Postal Service in February 2001 from the San Mateo, CA, Health Department to Microbiological Disease Laboratory in Berkeley, CA. She said the package was mishandled and the vial of meningitis somehow ended up in the daughter's package. Meningitis affects the brain and spinal cord and is fatal in approximately 10 percent of cases. The family discovered the biohazard

canister May 31, 2001. They called the county Health Department, which sent someone to check it out. Health officials called two days later and said they had been in no danger. The package tested negative for meningitis. The Neisseria meningitis sample was so old it was probably harmless, and there was no evidence it had leaked, officials said.
Source: http://www.santacruzsentinel.com/archive/2005/June/17/local/ stories/02local.htm

[Return to top]

Agriculture Sector

18. *June 17, CBC News (Canada)* — **Company says it has developed new mad cow test.** A Calgary company says it is developing a test that will detect mad cow disease, also known as BSE, in the blood of live cattle, which would prevent the unnecessary slaughter of animals that don't have the disease. Right now, if an animal is suspected of having BSE, it must be killed and its brain tissue tested for the wasting disease. The company says the test, which was developed in France, takes about 30 minutes and can be done for $20 an animal. The test looks for a protein marker that identifies whether BSE is present in the blood. Company president Bill Hogan says the French Food Safety Agency and the Veterinary Laboratories Agency in England provided samples of blood, some of which were positive for BSE, and others that were clean. The blood was then tested. He said it had a 96 percent success rate in detecting the disease.
Source: http://www.cbc.ca/story/canada/national/2005/06/16/bse−test0 50616.html

19. *June 17, Clovis Journal (NM)* — **Livestock identification system in testing.** New Mexico ranching industry leaders are finding ways to track their animals with advances in technology such as the National Identification System which is in its early stages within the state. The Tri−National Animal Health and Identification Consortium recently launched a pilot series to test the new livestock identification system on Quay County 4−H and FFA livestock, which will allow the Department of Agriculture to trace an animal to any registered location it has visited since it was entered into the system. An ear tag the size of a bottle cap containing an antennae is stamped into the animal's ear. The tag is scanned with a wand, a device similar to a small hand−held metal detector used by airport security. The ID number scanned is later logged into a database compiled by the U.S. Department of Agriculture (USDA). While the Tri−National Consortium is actuating the pilot program under state regulations, the ID program will be a national procedure mandated by the USDA by January 2009. The Consortium is asking livestock producers to register their premises, sites that will contain their livestock at any point in time whether it be a ranch, auction, or grazing allotment.
Source: http://cnjonline.com/engine.pl?station=clovis&template=story full.html&id=11655

20. *June 16, Associated Press* — **Mad cow sample is hand−carried to England.** A U.S. Department of Agriculture (USDA) official left Thursday, June 16, for England carrying brain tissue samples from a cow suspected of having mad cow disease. The cow was declared free of the infection seven months ago, but the USDA did further tests last week that came back positive. The samples are destined for the internationally recognized laboratory in Weybridge, England, that gave independent confirmation of the first U.S. case of mad cow disease in December 2003. The lab will perform a combination of tests already done in the U.S., said John Clifford, the USDA's chief veterinary officer. More analysis will also be done at the National

Veterinary Services Laboratory in Ames, IA, he said.
Source: http://seattlepi.nwsource.com/national/apscience_story.asp?category=1500&slug=Mad%20Cow

21. *June 16, Agence France Presse* — **Foot−and−mouth disease enters Russia from China.** Foot−and−mouth disease has crossed from China into Russia's Far East, forcing a trade ban on the infected Amur region. The outbreak of the disease was registered in the village of Busse, where an immediate quarantine was enforced, regional emergency ministry officials said Thursday, June 16. Foot−and−mouth disease is a highly contagious illness that affects cows, sheep, pigs, and horses.
Source: http://news.yahoo.com/s/afp/20050616/hl_afp/russiachinahealthfarm_050616144113;_ylt=AglCTclPbRqrBTryKwI.S7SJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Food Sector

22. *June 16, Canadian Press* — **Pandemic could cause food shortages, expert warns.** An influenza pandemic would dramatically disrupt the processing and distribution of food supplies across the world, emptying grocery store shelves and creating crippling shortages for months, an expert warned Thursday, June 16. Michael Osterholm, director of the Center for Infectious Disease Research and Policy at the University of Minnesota, suggested policy makers must start intensive planning to figure out how to ensure food supplies for their populations during a time when international travel may be grounded or severely cut back, when workers are too sick to process or deliver food, and when people will be too fearful of disease to gather in restaurants. Osterholm said the "just−in−time" delivery model by which modern corporations operate means food distribution networks don't have warehouses brimming with months worth of inventory. Most grocery store chains have only several days worth of their most popular commodities in warehouses, he explained, with perhaps 30 days worth of stock for less popular items. He pointed to the short−term shortages that occur when winter storms threaten communities, then suggested people envisage the possibility of those shortages dragging on for somewhere between 18 months and three years as the expected successive waves of pandemic flu buffet the world.
Source: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1118969974296_47/?hub=Health

[Return to top]

Water Sector

23. *June 15, American Water Works Association* — **National Drinking Water Advisory Council identifies active and effective practices for securing water supplies.** A new report from the National Drinking Water Advisory Council will help utilities implement security practices and measure their effectiveness, security experts announced at the American Water Works Association's Annual Conference and Exhibition (ACE 05) last week. "This report is a

significant step in our quest to assure a culture of security at water systems throughout North America," said J. Alan Roberson, AWWA director of security and regulatory affairs. "The recommendations establish a consistent expectation for what features constitute an 'active and effective' water security program, but it does so in a way that allows utilities flexibility based on their size and local circumstances." The report describes the framework that large and small, urban and rural utilities can implement to provide their communities with safe and secure systems. In addition to identifying practices essential to effective security programs, the report developed findings on incentives to encourage security practices and measures to gauge their effectiveness.
Report: http://www.awwa.org/Advocacy/govtaff/govnew.cfm
Source: http://www.awwa.org/Advocacy/pressroom/pr/index.cfm?ArticleI D=453

[Return to top]

Public Health Sector

24. *June 17, Bloomberg* — **FDA approves new antibiotic.** Wyeth said Thursday, June 16, that it had won federal regulatory approval to sell Tygacil, the first of a new class of antibiotics able to fight infections that outwit treatment with existing medications. The intravenous drug treats a wide variety of potentially fatal infections, including those caused by E. coli bacteria. Tygacil was approved for stomach and skin infections, including burns, ulcers, and abscesses and may be given even before doctors determine what bacteria is responsible, Wyeth said. About 70 percent of the two million infections among hospitalized Americans each year are resistant to one or more drugs, driving up the cost and complexity of care, according to the Infectious Diseases Society of America. Tygacil may change the way doctors treat intensive−care patients, doctors said. The Food and Drug Administration (FDA) approval is the first for Tygacil, part of a new class of medicines called glycylcyclines. The drug is under review elsewhere in the world, including Europe, Canada, Mexico, and Taiwan.
Source: http://www.nytimes.com/2005/06/17/business/17wyeth.html?oref =login

25. *June 17, Wichita Eagle (KS)* — **West Nile emerges in Kansas.** Kansas has the nation's first human case of West Nile virus this year. The Kansas Department of Health and Environment (KDHE) said Thursday, June 16, that a 51−year−old in Douglas County had West Nile virus symptoms. The U.S. Centers for Disease Control and Prevention hasn't had any other reports of West Nile virus in humans yet this year, a spokesperson said, though other states have reported it in birds, animals, and mosquitoes. It is the first West Nile case of any kind in Kansas this year. This is the earliest in the mosquito season that West Nile has been reported in humans in Kansas. In previous years, human cases started showing up in late July or August, several weeks after the virus had been detected in mosquitoes and birds. KDHE said the person in Douglas County developed symptoms in mid−May.
Source: http://www.kansas.com/mld/kansas/living/11916467.htm

26. *June 16, Associated Press* — **Massachusetts hospitals investigate tuberculosis exposure.** Four Massachusetts hospitals are asking hundreds of patients and staff to be tested for tuberculosis (TB) after learning a worker was diagnosed with the disease, health officials said. Authorities said Thursday, June 16, that the female surgical resident was contagious for six months and may have exposed more than 2,000 patients at the hospitals. She had shown

symptoms of a chest infection in December, but the TB wasn't confirmed until Monday, June 13. Hospital officials are contacting patients who came in direct contact with the woman and requiring testing for employees who had close contact while the woman worked at Boston Medical Center, the Veterans Affairs hospital's West Roxbury campus, Brockton Hospital, and Cape Cod Hospital. Boston Medical Center is requiring 750 of its roughly 4,000 employees to be tested. At least one−third of the 3,000 workers at the West Roxbury hospital also will be tested. John Rich, medical director at Boston Public Health Commission, which is leading the investigation, said patients have a lower risk of becoming infected than the woman's co−workers, who spent more time with her. But officials said it could be weeks, if not months, before they know whether any others have been infected.
Source: http://www.boston.com/news/local/massachusetts/articles/2005/06/16/4_mass_hospitals_investigate_tb_exposure/

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

27. *June 17, Government Technology* — **Atlanta police and fire departments improve 911 communications.** New signals and codes have been implemented between the Atlanta Police Department and the Atlanta Fire Rescue Department. Police and fire will now have one set of 911 signals and codes to communicate with one another. The codes and signals will be in what is known as "plain talk", or communicating without the signals and the use of words that make it easy to understand the emergency. Currently, there are 95 signals and 34 codes used by police and fire. Prior to the consolidation there were 95 fire signals, 91 police signals, three fire codes and 31 police codes. The new codes and signals are helping to enhance the efficiency of dispatchers who send calls to fire and police personnel, while also creating a more accurate compilation of statistical data.
Source: http://www.govtech.net/news/news.php?id=94318

28. *June 17, Tucson Citizen (AZ)* — **Terror response training in Arizona.** One hundred firefighters will graduate today from a program that is part of the Arizona's terror response plan. In January, the Tucson, AZ Fire Department received two million dollars to cover training in hazardous materials and technical rescue, in addition to covering the cost of two Rapid Response Team (RRT) trucks. Tucson Fire Department Captain Paul McDonough said the two Tucson units will be among 11 units across the State with the ability to respond to major incidents either locally or statewide. A pamphlet about the program says each RRT unit will be trained and equipped to handle structural collapse, technical rescue, fire suppression, mass casualty, and hazardous−materials incidents. Each RRT has a six−person crew: a captain, engineer, two paramedics and two firefighters. The new RRT trucks will carry equipment for both hazardous materials and rescues. McDonough said the units will be effective in Tucson once the equipment arrives in July.

Source: http://www.tucsoncitizen.com/index.php?page=local&story_id=061705a6_firegraduation

29. *June 17, Burlington County Times (PA)* — **Moorestown ready if disaster strikes.** Emergency responders in Moorestown, PA, are preparing teams of residents to help them in times of need. The first Moorestown Community Emergency Response Team, or CERT, will graduate on Saturday, June 18 after members showcase their newly acquired skills. Moorestown joins other Burlington County, PA towns, including Evesham, Mount Laurel and Willingboro, which have organized the all−volunteer teams. The CERT members have attended one class per week for the past seven weeks, training in basic emergency skills, including fire, first aid, search and rescue and terrorism awareness. The classes also gave the team members a chance to familiarize themselves with township emergency operations and personnel. The Police Department can now activate the new team when needed, Parker said. For example, the CERT could assist authorities in natural disasters, performing such duties as evacuating residents and helping with traffic control, as well as in terrorism−related incidents. "They are another resource we have in case of an emergency," Parker said. The CERT program was created in the 1980s in California as a way to assist emergency officials during natural disasters such as earthquakes.
Source: http://www.phillyburbs.com/pb−dyn/news/112−06172005−503877.h tml

30. *June 17, Independent Online* — **Grant awarded to help update emergency communications in Ohio.** By the end of the year, every police and fire department in Stark County, OH, will be armed with the equipment needed to communicate with each other during a crisis. County commissioners on Thursday authorized the purchase of approximately 900 radios to be used as part of a countywide communications system. A $3 million federal grant will provide funding to supply the radios to safety forces throughout the county. “The biggest complaint of 9/11 was the lack of communication. Here we are solving a huge problem,” said Stark County Commissioner Gayle Jackson. Plans for a countywide system intensified following a tornado that ripped through Jackson, OH, in May 2002, during which safety forces were forced to relay messages to each other through the Regional Emergency Dispatch Center. This incident emphasized the need for various agencies to have the capability to communicate with each other in crisis situations. Upgrades to the Sheriff Department’s 800 megahertz system have already been completed. However, the system will only be used during emergencies due to lack of tower sites or frequencies to be able to operate 24/7 with all fire and police departments.
Source: http://www.indeonline.com/left.php?ID=3125&r=0&Category=1

31. *June 16, National Incident Notification Network* — **Tsunami warning systems failed in Washington State.** One of the major ways of alerting Washington State coastal residents to a tsunami −− the NOAA weather and hazard alert radio −− failed during the West Coast warning on Tuesday night, June 14. The meteorologist in charge of the National Oceanic and Atmospheric Administration (NOAA) office in Seattle, WA said the warning did not get disseminated because a phone line was out between the office and the Coast Guard. George Crawford of the State Department of Emergency Management stated that coastal residents should have been evacuated. In LaPush, WA, Police Chief Bill Lyon said that when the warning siren failed to go off automatically, he activated it by hand. He said officers and firefighters then evacuated more than 600 residents to higher ground. Police Chief T.J. Green of Neah Bay, WA, said a recently installed tsunami siren in the area did not go off. The warning

was eventually downgraded after officials determined there was no wave generated by the quake off Northern California.
Source: http://newscenter.ninn.org/modules.php?name=News&file=articl e&sid=11274

[Return to top]

Information Technology and Telecommunications Sector

32. *June 17, Zone−H.org* — **Adobe Reader 7 vulnerable to XML External Entity (XXE) attack.** Recent versions of Adobe Reader are vulnerable to XML External Entity (XXE) attacks. By including a JavaScript in a PDF file, and having this JavaScript parse an embedded XML document with a reference to an external entity, it is possible to read certain types of text files on the local computer, and have them sent to a remote attacker. Original advisory and updates available: http://www.adobe.com/support/techdocs/331710.html
Source: http://www.zone−h.org/advisories/read/id=7674

33. *June 16, SecurityFocus* — **Ultimate PHP Board weak password encryption vulnerability.** Ultimate PHP Board is prone to a weak password encryption vulnerability. This issue is due to a failure of the application to protect passwords with a sufficiently effective encryption scheme. This issue may allow a malicious user to gain access to user and administrator passwords for the affected application. There is no solution at this time.
Source: http://www.securityfocus.com/bid/13975

34. *June 16, SecurityFocus* — **Gedit filename format string vulnerability.** gEdit is prone to a format string vulnerability. Exploitation may occur when the program is invoked with a filename that includes malicious format specifiers. This issue could be exploited to corrupt arbitrary regions of memory with attacker supplied data, potentially resulting in execution of arbitrary code in the context of the user running the program. See Source link below for vendor updates.
Source: http://www.securityfocus.com/bid/13699/solution

35. *June 16, SecurityFocus* — **Opera cross site scripting and security bypass vulnerabilities.** Multiple vulnerabilities were identified in Opera, which may be exploited by malicious Websites to conduct cross−site scripting attacks. The first flaw is due to insufficient validation of server side redirects when handling "XMLHttpRequest" objects, which could be exploited to access resources from outside the domain of which the object was opened. The second vulnerability is caused due to Opera not properly restricting the privileges of "javascript:" URLs when opened in e.g. new windows or frames which could be exploited to conduct cross site scripting attacks and to read local files. The third issue exists in the way the Opera browser generates a temporary page for displaying a redirection when "Automatic redirection" is disabled (not default setting), which could be exploited to conduct cross site scripting attacks. Update to Opera 8.01: http://www.opera.com
Source: http://www.securityfocus.com/bid/6962/solution

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports Microsoft Security Bulletins for June, 2005 address a number of vulnerabilities in Windows, Internet Explorer, Outlook Express, Outlook Web Access, ISA Server, the Step by Step Interactive Training engine, and telnet. Exploitation of the most serious of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. This would allow an attacker to take complete control of a vulnerable system. An attacker could also execute arbitrary code with user privileges, or cause a denial of service. Further information about the more serious vulnerabilities is available at URL: http://www.us−cert.gov/cas/techalerts/TA05−165A.html Activity on one of the ports associated with Windows' Server Message Block (SMB) protocol is climbing. A surge in activity targeting TCP port 445, which is associated with SMB−related communications on Windows machines has been observed. This may indicate an increase in known attacks, such as password brute forcing, or the exploitation of known vulnerabilities, or may indicate activity related to the recent Microsoft Incoming SMB Packet Validation Remote Buffer Overflow Vulnerability

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 6881 (bittorrent), 27015 (halflife), 1026 (−−−), 139 (netbios−ssn), 9442 (−−−), 53 (domain), 1434 (ms−sql−m), 137 (netbios−ns) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

36. *June 18, New Haven Register (CT)* — **Police believe an adult wrote threatening school note.** Handwriting analysis led police Friday, June 17, to conclude that the person responsible for a threatening note about Milford, CT, city schools is likely an adult, and authorities were investigating whether the writer also called bomb threats into Jonathan Law High School. The bomb threats forced the evacuation of the school Thursday, June 16. The caller who made the threats against the schools had initially named Thursday as his target, then switched the threat to Friday. Police continue to treat the threats very seriously. Based on handwriting analysis, investigators believe an adult wrote the note, in part because the envelope contained the word "CONN" as an abbreviation for Connecticut, a style not taught in the schools for more than a decade, police spokesperson Officer Vaughan Dumas said. The handwriting also contains some swirls on letters, and letters were all capitalized, also not taught in the school system, he said. Dumas reiterated patrols have been increased around all 14 city schools, and officers are at all

the schools. He promised additional resources would be deployed through the last day for school.
Source: http://www.nhregister.com/site/news.cfm?newsid=14717181&BRD=1281&PAG=461&dept_id=517515&rfi=6

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original

copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.